REMARKS

Claims 1-4, 7-11, 13-16, and 19-20 are pending with claims 1, 8, and 13 being independent. Claims 1, 8, and 13 are being amended. Support for the amendments is found throughout the specification, as described more specifically below. Applicants respectfully request reconsideration of the pending claims in view of the amendments and the following remarks.

Interview Summary

Applicants thank Examiner Zee for participating in the interview on Thursday, August 20, 2009. The interview included a discussion of the claimed subject matter and the rejections under 35 U.S.C. §§ 101, 112, and 103. The Examiner indicated that the above claim amendments would overcome the § 101 rejections and the § 112 rejections. The interview included a discussion of the distinctions between the claimed subject matter and the Wong and Kraenzel references. Applicants and the Examiner discussed amendments to better distinguish the references from the claims. Applicants noted that the amendments incorporated subject matter that the Examiner had previously indicated was allowable in a January 1, 2009 Office Action. The Examiner appeared to agree that the amendments overcame the § 103 rejections, but indicated that further search and consideration may be necessary.

Claim Rejections – 35 U.S.C. § 101

The Office Action (at page 3) rejected claims 8-11 because the claimed invention was allegedly directed to non-statutory subject matter. Specifically, the Office Action asserted that a statutory process under 35 U.S.C. § 101 must (1) be tied to a particular machine, or (2) transform underlying subject matter. The rejections are moot as the claims are amended, but the Applicants are not conceding that the rejection had merit. Amended independent claim 8 recites a permission object "included in a storage object" and that a user is permitted to access any of the requested attributes "using a processor." The Examiner agreed during the August 20

interview that the amendments overcame the rejections under 35 U.S.C. § 101. Dependent claims 9-11 are patentable for at least the same reasons as independent claim 8. Applicants respectfully request that the rejections under 35 U.S.C. § 101 be withdrawn.

Claim Rejections – 35 U.S.C. § 112

The Office Action (at page 2) rejected claims 1-4, 7-11, 13-16, 19-20 under 35 U.S.C. § 112, second paragraph, as being allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action asserted the "the attribute" in line 26 of claim 1 (as amended in the last response), "the data object that the user seeks to access" in line 26 of claim 1, and "the attribute sought to be accessed in lines 31-32 of claim 1 had insufficient antecedent basis. The rejections are moot as the claims are amended, but the Applicants are not conceding that the rejection have merit. The Examiner agreed during the August 20 interview that the amendments overcame the rejections under 35 U.S.C. § 101. Independent claims 8 and 13 recite similar language and are patentable for at least the same reasons as independent claim 1. Dependent claims 2-4, 7, 9-11, 14-16, 19, and 20 are patentable for at least the same reasons as their independent claims. Applicants respectfully request that the rejections under 35 U.S.C. § 112 be withdrawn.

Support for Claim Amendments

The Examiner requested during the August 20 interview that Applicants direct the Examiner to portions of the specification that provide support for the discussed amendments. Applicants note that support can be found throughout the specification. As an example, support for the attribute access group having a "subset of attributes being fewer than all of the multiple attributes" in the attribute access group can be found throughout the specification, for example, in FIG. 4. The customer attribute group 423 is a subset of all attributes 422 in the business object 420.

Support for "wherein the permission object is configured to use the permission attribute included in the attribute access group and to use the permission attribute not included in the

attribute access group" can be found throughout the specification, for example, at FIG. 4 and at page 14, lines 19-30. In FIG. 4, the permission filters 424 and 428 are not included in the attribute groups 423 and 426, respectively. Page 14 describes an example where a permission attribute is for a "Region" attribute, and a user is provided access to a set of attributes (row 33A) that includes the "Region" attribute.

Support for permitting the user to access "any of the requested attributes indicated by the attribute access group and not permitted to access any of the requested attributes not associated with the attribute access group" can be found throughout the specification, for example, at page 18, lines 20-23. Applicants respectfully request that the Examiner call Applicants' undersigned representative if the Examiner has any concerns about the support for the above amendments.

Claim Rejections – 35 U.S.C. § 102

The Office Action rejected claims 1-4, 7-11, 13-16, and 19 under 35 U.S.C. § 102(e) as being allegedly anticipated by Wong et al. (U.S. Patent No. 6,578,037). Alternatively, the Office Action rejected claims 1-4, 7-11, 13-16, and 19 under 35 U.S.C. § 102(b) as being allegedly anticipated by Keisuke et al. (EP 0992 873 A2). Applicants respectfully submit that Wong and Keisuke each fail to disclose at least one element of pending claims 1-4, 7-11, 13-16, and 19.

In general, the subject matter of the present application relates to a system that grants access to information. Access can be governed by a set of "permission objects" that are each particular to a user affiliation (e.g., a "sales" user group) and data object type (e.g., an "employee records" type of object). For example, if there are two user affiliations and three data object types, the system may have six permission objects, one for each combination. Aside from specifying the user group and data object type to which the permission object applies, each permission object defines additional criteria including (a) a permission attribute, (b) a permission value, and (c) an attribute access group.

The permission attribute can identify a specific attribute from among those common to data objects of the specified type. The specific attribute in each purchase order contains a value that determines if access is granted to attributes in a particular data object. The permission value

can be the values in the specified attribute that result in user access being provided. The attribute access group can identify a subset of the attributes in the data object as those that the user is provided access to if the criteria are met. The permission attribute can be an attribute that is part of the attribute access group, or not part of an attribute access group. The inclusion of an attribute access group and permission attribute in each permission attribute can provide users access to different sets of attributes in data objects of a specific type based on the user affiliation. Access to the set of attributes can be granted based on any of the attributes in the data objects.

Claim 1 recites a computer-readable medium storing code segments configured to

use a permission object to determine whether a user associated with an entry in user information is permitted to access requested attributes of a data object associated with a data object type, wherein:

the entry in the user information associates the user with a user affiliation,

the permission object identifies:

a user affiliation to which the permission object applies,

a data object type to which the permission object applies such that the data object type identified by the permission object is associated with multiple attributes and each data object having the data object type identified by the permission object is associated with the multiple attributes,

a permission attribute identifying at least one of the multiple attributes,

a permission value for the permission attribute, and

an attribute access group having a subset of attributes of the multiple attributes, the subset of attributes being fewer than all of the multiple attributes, wherein the permission object is configured to use the permission attribute included in the attribute access group and to use the permission attribute not included in the attribute access group,

wherein upon determination that:

(1) the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the permission object applies,

(2) the data object type of the data object is the same as the data object type to which the permission object applies,

(3) a value of the permission attribute associated with the data object is consistent with the permission value for the permission attribute, and

(4) at least one of the requested attributes of the data object corresponds to an attribute of the attribute access group of the permission object,

the user is permitted to access any of the requested attributes indicated by the attribute access group and not permitted to access any of the requested attributes not associated with the attribute access group, and wherein otherwise the user is denied access to all the requested attributes.

Regarding independent claim 1, Wong fails to teach "***an attribute access group having a subset of attributes of the multiple attributes [of a data object type]***" where "***the user is permitted to access any of the requested attributes indicated by the attribute access group and not permitted to access any of the requested attributes not associated with the attribute access group***" upon certain criteria being fulfilled. In contrast, Wong describes a system that either grants access to entire employee records or denies access to entire employee records depending on a salary of each individual employee. (Wong, at col. 6, lines 23-48.) Even if each individual employee record were a data object of a specific type (an issue Applicants do not concede), Wong does not describe a system that defines for the employee records "an attribute access group having a ***subset*** of attributes" of each employee record, where the subset of attributes are those attributes that "the user is permitted to access" if specific criteria are met. Wong provides access to the entire employee record, not a subset of the record.

Keisuke also fails to teach the recited subject matter. The Office Action (at pages 11 and 12) assert that FIG. 16 and pars. [0142]-[0146] teach the recited subject matter. Contrary to the recited subject matter, FIG. 16 shows an "access-right setting pattern group" that grants to individual "ranks" of users specific forms of access rights to an ***entire server***. More specifically, "[a]fter the users registered in the user information 26 have been assigned rights to access the content 28, they are allowed to access the content 28 in the WWW server 13 in each of the departments 3, 4, in the range of access-rights assigned to them." (Keisuke, at par. [0142].) Figure 16 shows a table that can assigned, for different ranks of users" a combination of "read rights" and "vote rights" for the WWW servers. The table in FIG. 16 does not include an attribute access group. Even if Keisuke's WWW servers were a data object of a particular type (an issue Applicants do not concede), Keisuke grants access to the entire WWW server. Keisuke does not include a permission object that is specific to the WWW server and a user affiliation,

where the permission object include an attribute access group that defines a subset of attributes in the WWW server which users can access.

Regarding independent claim 1, Wong fails to teach a permission object that is "***configured to use the permission attribute included in the attribute access group and to use the permission attribute not included in the attribute access group***." As noted above, Wong fails to teach an attribute access group. For at least this reason, Wong also fails to teach a system that can use a permission attribute as either included in the attribute access group or outside of the attribute access group. An advantage of the recited subject matter is that a user can be granted access to a particular record based upon a value of an attribute that is either accessible to the employee upon gaining access, or non-accessible to the employee upon gaining access.

As an exemplary and non-limiting example, suppose an "employee records" data object type is associated with the attributes "Name," "Position," "Length of Service" and "Employee ID." An attribute access group in a permission object for the "employee records" data object and a "Students" user affiliation may include the attributes that students are permitted to access (e.g., "Name" and "Position"). In other words, if granted access to an employee record, the students cannot see the employee's "Length of Service" and "Employee ID." The permission attribute (i.e., the attribute that is checked to determine if a student can access the employee record), can either be within the attribute access group or outside of the attribute access group. For example, the permission attribute can be "Position" (which is in the attribute access group) or "Length of Service" (which is outside of the attribute access group). If "Position," students may only be able to see records for "Positions" that are "Teachers" and not "Janitors." If "Length of Service," students may only be able to see records for employees that have worked at the school for more than 5 years.

Keisuke also fails to teach the recited subject matter. As noted above, Keisuke fails to teach an attribute access group. For at least this reason, Keisuke also fails to teach a system that can use permission attribute as either included in the attribute access group or outside of the attribute access group.

Accordingly, Wong and Keisuke each fail to teach each and every element of independent claim 1. Independent claims 8 and 13 include similar language and are patentable for at least the same reasons. Dependent claims 2-4, 7, 9-11, 14-16, and 19-20 are patentable for at least the same reasons as their independent claims, and for the independently patentable features recited therein.

Claim Rejections – 35 U.S.C. § 103

The Office Action (at page 10) rejected claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Wong in view of Kraenzel. Applicants respectfully submit that claim 20 depends from independent claim 1 and is patentable for at least the same reasons as claim 1, and the independently patentable features recited therein.

Conclusions

Claims 1-4, 7-11, 13-16, and 19-20, as amended, appear to be in form for allowance. As such, Applicants request that the Examiner allow claims 1-4, 7-11, 13-16, and 19-20.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date:September 15, 2009_____

/j richard soderberg reg. no. 43,352/_____
J. Richard Soderberg
Reg. No. 43,352

Fish & Richardson P.C.
3200 RBC Plaza
60 South Sixth Street
Minneapolis, Minnesota 55402
Telephone: (612) 335-5070
Facsimile: (877) 769-7945